REMARKS/ARGUMENTS

The **First Issue** is whether the Examiner is justified in rejecting claims 1-3 and 10-11 under 35 USC 103(a) as being unpatentable over a three-way combination of:

- Ben Laurie, Configuration file for Apache-SSL (URL provided by the Examiner in the Office Action), hereinafter "Laurie", and
- AOL Server, Server configuring (URL provided by the Examiner in the Office Action), hereinafter "AOL", and
- Apache (URL provided by the Examiner in the Office Action), hereinafter "Apache",

despite:

(1-a) Laurie's, AOL's and Apache's failure to disclose

(1-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol,

(1-a-2) configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP, and

(1-a-3) configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443;

(1-b) Laurie's, AOL's and Apache's teaching away from

(1-b-1) configuring an HTTPS server to use a port normally associated with some other service;

(1-c) the fact that

(1-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(1-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(1-c-3) for several years after Applicant first reduced Applicant's invention to practice and for several years since Laurie was written, others who are skilled in

the art did not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem as defined below at 1-c (i.e., how to communicate securely through a firewall that blocks outgoing packets with a destination port of 443), and

(1-c-4) the Examiner failed to describe modifications to Laurie that in the view of the examiner both (i) would bring Laurie within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Laurie and was confronted by the Firewall Problem; and

(1-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

To understand the following discussion, it is useful to remember that when a web browser program running on a client computer sends to a web host computer a packet requesting a new session, the sent packet typically includes, among other things, a destination port number. The destination port number is the port number where the client computer hopes the host will be listening for session requests of the type that the client computer is making in the sent packet.

Normally, if the client computer wishes to establish a HTTP session with the host, the client computer will specify a Destination TCP (transmission control protocol) Port of 80. Note that for many browser programs a URL of the form http://www.domain.com implies port 80 and is equivalent to a URL of the form http://www.domain.com:80 .

Normally, if the client computer wishes to establish a HTTPS session with the host, the client computer will specify a Destination TCP Port of 443. Note that for many browser programs a URL of the form https://www.domain.com implies port 443 and is equivalent to a URL of the form https://www.domain.com:443 .

One embodiment of Applicant's invention concerns configuring a web server to listen for requests for HTTPS sessions on port 80 (rather than port 443) and then directing a web browser to send requests for HTTPS sessions to port 80 (rather than port 443),

thereby permitting encrypted communications through firewalls near the client computer that block communication to ports other than port 80. For example, by directing a browser to request a URL of the form https://www.domain.com:80.

(1-a) Laurie's, AOL's and Apache's failure to disclose required elements of claims 1-3 and 9-11.

(1-a-1) Laurie, AOL and Apache fail to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by (i) Claim 1 step (a) (upon which claims 2-3 and 9 depend), (ii) Claim 10 step (a) and (iii) Claim 11 element (a).

To the contrary, Laurie teaches away from Applicant's invention. Laurie teaches configuring a server program to listen for requests for secure hypertext transfer protocol sessions on port 8887, a port number not normally associated with any protocol or server, much less a hypertext transfer protocol (as expressly required by the above referenced claims).

In the Office Action at page 3, line 12, the Examiner admits that Laurie "... is silent on the second port as the http port or port 80."

In an attempt to overcome this "problem" with Laurie, the Office Action at page 3, lines 13-14, refers to portions of AOL that either are irrelevant to Applicant's invention or teach away from Applicant's invention.

Irrelevant. Applicant's invention neither requires, nor prohibits, the operation of a server for a non-secure hypertext transfer protocol on the same computer as the secure hypertext transfer protocol with which Applicant's invention is concerned. Consequently, the manner in which a server for a non-secure hypertext transfer protocol might be configured is irrelevant to Applicant's invention.

Teaches Away. AOL teaches configuring a server program to listen for requests for a non-secure hypertext transfer protocol (i.e., HTTP) on port 9876, a port number not normally associated with any protocol or server, much less a hypertext transfer protocol (as expressly required by the above referenced claims).

In the Office Action at page 3, lines 18-19, the Examiner admits that "... neither Laurie nor AOL discloses a method of modifying the https port (443) to listen on a second port http port (80)." [Emphasis added.] This comment is a bit "off the mark", because the claims at issue require setting the port number associated with a secure hypertext protocol to a particular value, rather than requiring that some specific method be used to implement such a change. As an analogy, if a reference should disclose the general method of sand casting, it would not thereby disclose all articles that might possibly be manufactured using the sand casting method.

In an attempt to overcome the fact that both Laurie and AOL teach away from the Invention (by teaching configuring a secure HTTPS server to listen on an otherwise unassigned port [Laurie] or by teaching configuring a non-secure HTTP server to listen on an otherwise unassigned port [AOL]), the Examiner, in the Office Action at page 3 line 19 – page 4 line 6, says that Apache discloses a method of changing the ports associated with both an HTTPS and an HTTP server. The Examiner argues that Laurie in light of AOL and Apache would have made it obvious how to configure an HTTPS server to listen on port 80. However, the Examiner offers no real explanation about why someone skilled in the art at the time of Applicant's invention wishing to communicate through a firewall would have been likely to combine the teachings of Laurie, AOL and Apache in the manner hinted at by the Examiner.

In the interest of efficiency, Applicant once again admits that at the time of Applicant's invention it was well known by those skilled in the art how to configure Microsoft's Internet Information Server to listen for requests for https sessions

on any desired port. See for example the Application as published at page 12 paragraphs 0239-0242 which include instructions for configuring an https server to listen on port 80.

However, Applicant continues to believe that configuring an HTTPS server to listen on port 80 was non-obvious at the time of Applicant's invention.

Applicant contends that if, at the time of Applicant's invention, a programmer skilled in the art had encountered difficulty communicating from a browser program, through a firewall that blocked access to ports other than 80, to an HTTPS server listening on port 443, it would not have been obvious for such a programmer to (i) start with Laurie (which teaches configuring an HTTPS server to use non-standard port 8887 [which also would be blocked by firewalls that block access to ports other than 80]), (ii) decide that Laure offers some sort of help solving the problem (for goodness knows what reason), (iii) think of combining Laurie with AOL (which teaches configuring an HTTP server to use non-standard port 9876 [which for firewalls that block access to ports other than 80 would have the effect of "breaking" HTTP which otherwise would have worked while assigned to port 80]), (iv) decide that combining Laurie and AOL might somehow be useful (even though Laurie provided no obvious help and AOL seemed to make the problem worse), (v) think of combining Laurie and AOL with Apache, and (vi) finally, contrary to the teaching of Laurie, AOL and Apache, configure the HTTPS server to listen on port 80.

(1-a-2) Laurie fails to disclose configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP, as (i) required by Claim 2 and (ii) contemplated by Claims 10 and 11. Since HTTPS is an example of a secure hypertext transport protocol and HTTP is an example of a Hypertext Transport Protocol, the general discussion above for item 1-a-1 is fully applicable here.

(1-a-3) Laurie fails to disclose configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443, as (i) required by Claim 3 and (ii) contemplated by Claims 10 and 11. Since HTTPS is an

example of a secure hypertext transport protocol that normally uses port 443 and HTTP is an example of a Hypertext Transport Protocol that normally uses port 80, the general discussion above for item 1-a-1 is fully applicable here.

(1-b) Laurie, AOL and Apache teach away from elements of Claims 1-3 and 10-11.

(1-b-1) Laurie, AOL and Apache teach away from configuring a server to listen on a port that is normally associated with some other protocol or server.

Laurie teaches configuring HTTPS to listen on port 8887, which has no normal association.

AOL teaches configuring HTTP to listen on port 9876, which has no normal association.

Apache teaches configuring HTTPS to listen on port 443, rather than a port that is normally associated with some other protocol. In particular, Apache at Page 2 /etc/service (the portion cited by the Examiner) teaches associating https with port 443, its default port.

(1-c) As discussed in the Application as published on page 12 paragraphs 0232 – 0236, Applicant's invention seeks to solve the following problem (the "Firewall Problem"): how can a client computer use HTTPS to communicate securely with a server computer when such client computer is connected to the Internet through a firewall that blocks packets addressed to destination port 443 (the port number normally associated with HTTPS) but passes packets addressed to destination port 80.

The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem.

(1-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP).

A. The materials available at http://ftp.monash.edu.au/pub/ap/Apache/ch01.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch04.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch05.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch07.htm (hereinafter, collectively, "Apache Manual"), copies of which have already been provided by the Examiner and/or the Applicant, teach away from using port 80 for any protocol other than http and teach away from using ports 1-1024 as a nonstandard port for a server.

In Chapter 1 of Apache Manuals at Fig. 1.1 (page 3 of 11 when printed by Applicant), the www service (which uses http, the hyper text transfer protocol) is equated with port 80. This teaches away from the notion that port 80 should be used for other protocols, including without limitation SSL/https.

In Chapter 7 of Apache Manuals under the heading "Protecting Your Data from Outside Access" at "Caution" (which appears on page 29 of 38 when printed by Applicant), in the context of discussing how to hide a non-secure/http server, says in relevant part:

> "The second way to make your server less likely to be found is to run it on a nonstandard port. Ports can range from 0 to 65,535, so there is a wide range to choose from. Generally, the first 1024 are considered reserved ports."

By pointing out how many ports are potentially available and observing that the first 1024 are considered reserved ports, Apache teaches away

from moving any server to a non-standard port in the range from 0 to 1024. That range includes port 80 which is normally associated with HTTP / hyper text transfer protocol.

B. The Applicant previously filed a copy of Running a Perfect Web Site with Windows – Chapter 5, hereinafter "Windows (Chapter 5)" (from the web at http://www.gsu.unibel.by/pub/perf_web/06r07632.HTM).

The notice at the top of Windows (Chapter 5) says "Copyright © 1996" and is very similar to the notice at the top of Chapter 4 of Apache that was provided by the Examiner.

Windows (Chapter 5) at the bottom of page 3 says in relevant part:

> "… Ports under 1024 are reserved for the most common types of Internet traffic, so it is recommended that you use a number above 1024 if you need an alternate port. …"

(1-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. At the time of Applicant's invention, based upon materials such as Apache Manuals and Windows (Chapter 5), one skilled in the art would have expected that changing the port number on which an HTTPS server listens for session requests would make it harder for clients to communicate with such server. However, for clients connected to the Internet through certain types of firewalls, configuring an HTTPS server to listen on port 80 can make it possible for a client to establish an HTTPS session with such server in circumstances where it would not have been possible to establish an HTTPS session with such server if it were listening on port 443, the default port for HTTPS.

It is unexpected, serendipitous and counter-intuitive that configuring a server to listen to a non-standard and unexpected port would make it easier for some clients to reach such server, since this is precisely the sort of change that Apache

and Windows (Chapter 5) teaches will make it harder for browsers to communicate with the server.

The unexpected, serendipitous and counter-intuitive results obtained by practicing the Applicant's invention cut strongly against the Examiner's view that Applicant's invention was obvious at the time it was made.

(1-c-3) During the years that have passed since Applicant first reduced Applicant's invention to practice and the years that have passed since Laurie was written, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem (i.e., how to communicate securely through a firewall that blocks outgoing packets with a destination port of 443).

By rejecting Applicant's invention as obvious, the Examiner (in essence) contends that, at the time of Applicant's invention, it would have been obvious to one skilled in the art, when faced with the Firewall Problem addressed by Applicant's invention (i.e., that some clients are unable to communicate with a web server using HTTPS because such clients are connected to the Internet through a firewall that blocks packets to destination port 443), to configure the destination web server to listen for requests for HTTPS sessions on port 80 and to direct the affected clients' browsers to request information using a resource locator of the form "https://www.domain.com:80".

The technical staff of every e-commerce web site that attempts to do business with the general public ought eventually to encounter the Firewall Problem since some customers and some potential customers spend some time at offices or other locations where their computers are connected to the Internet through firewalls that block outgoing packets addressed to destination port 443.

Consequently, if Applicant's invention should be obvious to anyone skilled in the art who encounters the Firewall Problem, then it would be logical to expect that the technical staffs of many e-commerce web sites that seek to do business

with the general public would either (i) have duplicated Applicant's invention or (ii) have settled upon some other solution to the Firewall Problem that permits secure communication with affected customers' computers.

However, Applicant is not personally aware of any web sites that direct a customer's browser to a resource locator of the form https://www.domain.com:80 or implement some other solution to the Firewall Problem that permits secure communication with customers' computers that are affected by the Firewall Problem.

Consider for example the web sites barnesandnobel.com and amazon.com – two popular, highly competitive, technologically savvy e-commerce web sites that seek to conduct business with the general public.

Based on tests conducted by Applicant on December 13, 2005, it appears that when confronted with the Firewall Problem, the persons skilled in the art employed by barnesandnobel.com decided to drop back and punt. To ensure security, barnesandnobel.com used SSL (i.e., HTTPS) for order submission and the collection of credit card information. If the computer used by a potential customer of barnesandnobel.com is connected to the Internet through a firewall that blocks outgoing packets addressed to destination port 443, then the potential customer is allowed to fill up a shopping cart but at checkout time the potential customer's browser will display an unhelpful error message as soon as the customer's browser is directed to establish an HTTPS session using the default destination port of 443.

Based on tests conducted by Applicant on December 13, 2005, it is clear that when confronted with the Firewall Problem, the persons skilled in the art employed by amazon.com have also failed to duplicate Applicant's invention or to implement some different solution that permits encrypted communication with affected customers. The folks at amazon.com clearly recognize the Firewall Problem, warn customers about it, and offer affected customers the choice of giving up or submitting order and payment details in an unsecured manner (i.e., using HTTP rather than HTTPS).

In particular, the last page of the check out process that amazon.com normally sends to customers without encryption (i.e., using HTTP) contains both a button labeled:

"Sign in using our secure server"

and a link that says

> "The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server."

If a customer should click on the button labeled "Sign in using our secure server", then such customer's browser would be directed to a URL of the form "https://www.amazon.com/*", which by default implies destination port 443. If such customer's computer should be connected to the Internet through a firewall that blocks outgoing packets addressed to destination port 443 and such customer clicks on such button, then such customer would see an uninformative error message.

If a customer should click on the "standard server" link, then such customer's browser would be directed to a URL of the form "http://www.amazon.com/*" which by default implies destination port 80, thereby avoiding part of the Firewall Problem. Unfortunately, since that URL begins with "http", the remainder of the checkout process, including the transmission of credit card information, would then be conducted using HTTP which is NOT encrypted for security.

Since popular e-commerce sites that seek to do business with the general public neither (i) routinely use URLs of the form "https://www.securedomain.com/*:80" for the secure portions of their check out procedures nor (ii) routinely use some other solution to the Firewall Problem that ensures secure, encrypted communications with affected customers' computers, Applicant

contends that Applicant's invention was not obvious when it was first reduced to practice by Applicant and remains non-obvious today, years later.

(1-c-4) The Examiner failed to describe modifications to Laurie that in the view of the examiner both (i) would bring Laurie within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Laurie, AOL and Apache and was confronted by the Firewall Problem.

In the Office Action at page 3, line 12, the Examiner admits that Laurie does not teach configuring a server program to listen for requests for HTTPS sessions on a port number associated with the HTTP protocol (i.e., port 80) by stating:

> "However, LAURIE is silent on the second port as the http port or port 80."

In the Office Action at page 3, lines 13-14, the Examiner attempts to address this component of the obviousness issue with the following language:

> "Nevertheless, AOL teaches a method to modify the port of http port from the well-known HTTP port 80 to 9876 (Chapter 3 setup server, Page 1, 2nd paragraph). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to realize that LAURIE and AOL's teaching provide strong evidence that https's and http's ports are also operate-able at different ports or any port that is available."

After carefully reviewing the cited portions of both Laurie and AOL, it is not at all obvious to Applicant what modifications to Laurie in accordance with AOL would bring Laurie within the scope of any of claims 1-3 and 10-11. Two possible modifications to Laurie seem to be suggested by the cited portions of AOL:

First, perhaps the Examiner is suggesting that Laurie be modified to use for HTTPS the port suggested by AOL for HTTP. Modifying Laurie in

that way would result in associating port 9876 with the HTTPS server. Since port 9876 is not normally associated with any hypertext transfer protocol, Laurie as so modified would still be outside the relevant claims.

Second, perhaps the Examiner is suggesting that Laurie be modified to configure an HTTP server (as disclosed by AOL) rather than an HTTPS server (as disclosed by Laurie). Modifying Laurie in that way would result in associating port 8887 with the HTTP server. Modifying Laurie in that way would not involve associating the HTTPS server with a non-standard port, and thus Laurie as so modified would still be outside the relevant claims.

In the Office Action at page 3, lines 18-19, the Examiner admits that

> "... neither Laurie nor AOL discloses a method of modifying the https port (443) to listen on a second port http port (80)."

In the Office Action at page 3 line 19 – page 4 line 3, the Examiner attempts to address this component of the obviousness issue with the following language:

> "Nevertheless, Apache does discloses a method of configuring the /etc/services file to configure the port for each service, such as http and https (Page 2 /etc/services). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate LAURIE and AOL's teaching with Apache to modify the etc/services file so that http port will be listen at different port such as 9876 and https can be listen at port 80 (second port) instead of 443."

After carefully reviewing the cited portions of Laurie, AOL and Apache, it is not at all obvious to Applicant what modifications to Laurie in accordance with AOL and Apache would bring Laurie within the scope of any of claims 1-3 and 10-

11. As a matter of logic, no matter how many references show that a server can be associated with a non-standard port, if no reference discloses associating a server with a port that is normally associated with some other server, then no combination of such references discloses associating a server with a port that is normally associated with some other server.

(1-d) The Examiner has failed to provide any prior art to support a view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Laurie, in accordance with AOL and Apache, in a way that would bring Laurie within the scope of any of Claims 1-3 and 10-11. Applicant disagrees with the Examiner's view that it would be obvious to one of ordinary skill in the art to combine Laurie, AOL and Apache in a way that would bring Laurie within the scope of any of Claims 1-3 and 10-11. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges the Examiner's view and asks whether the Examiner can (i) describe a modification to Laurie in accordance with AOL and Apache that would bring Laurie within the scope of Claims 1-3 and 9-11 and (ii) show support for the view that it would have been obvious at the time of Applicant's invention for one skilled in the art so to modify Laurie upon encountering the Firewall Problem.

In light of the foregoing discussion, Applicant respectfully requests that claims 1-3 and 10-11 be allowed.

The **Second Issue** is whether the Examiner is justified in rejecting Claim 4 under 35 USC 103(a) as being unpatentable over Laurie as modified in accordance with AOL and Apache, despite:

(2-a) Laurie's, AOL's and Apache's failure to disclose

(2-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and

(2-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that

is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol;

(2-b) Laurie's, AOL's and Apache's teaching away from

(1-b-1) configuring an HTTPS server to use a port normally associated with some other service;

(2-c) the fact that

(2-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(2-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(2-c-3) during the several years since Applicant first reduced Applicant's invention to practice and the several years since Laurie was written, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem and

(2-c-4) the Examiner failed to describe modifications to Laurie that in the view of the examiner both (i) would bring Laurie within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Laurie and was confronted by the Firewall Problem; and

(2-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(2-a) Laurie fails to disclose elements of claim 4.

(2-a-1) Laurie fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by Claim 1 step (a), upon which Claim 4 depends. See the detailed discussion above at (1-a-1).

(2-a-2) Laurie fails to disclose receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed

through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol, as required by Claim 1 step (b) and Claim 4.

In the Office Action at page 4 lines 7-10, the Examiner admits this by stating:

> 'However, LAURIE is silent on "the first data packet is received by the server program on a second port, it passes through a system that is configured in a manner that would block the first data packet if the first data packet were addressed to the first port".'

The Examiner tries to address this issue by first saying:

> "Nevertheless, LAURIE does teach a process of modifying port so that the default service can only work on the set port (Page 1, 4th # bullet)."

Applicant has been unable to figure out how a portion of Laurie that teaches about changing the port on which an HTTPS server listens for packets can be viewed as disclosing anything about (i) a system that might block a packet if various conditions were satisfied or (ii) sending a packet through such a system on its way to an HTTPS server. Applicant is at a complete loss to see what in AOL or Apache would have suggested to one skilled in the art the addition to Laurie of such a conditional packet blocking system.

The Examiner then goes on to say:

> "Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to realize that the first port is no longer in service after modification."

Applicant respectfully submits that it is entirely irrelevant to Applicant's invention whether or not it would have been obvious for one skilled in the art to notice that an HTTPS server no longer responds to packets sent to port 443 after the HTTPS server has been reconfigured to listen for packets on port 8887. Applicant has not claimed the act of figuring out why there is no response to some packets. Even if it should have been easy at the time of Applicant's invention for one skilled in the art to realize that packets sent to port 443 were being blocked by a firewall, that realization would not have made it obvious to combine the method of Claim 1 with a firewall.

(2-b) Laurie, AOL and Apache teach away from elements of Claim 4.

(2-b-1) Laurie, AOL and Apache teach away from configuring a server to listen on a port that is normally associated with some other protocol or server.

Laurie teaches configuring HTTPS to listen on port 8887, which has no normal association.

AOL teaches configuring HTTP to listen on port 9876, which has no normal association.

Apache teaches configuring HTTPS to listen on its default port, rather than a port that is normally associated with some other protocol. In particular, Apache at Page 2 /etc/service (the portion cited by the Examiner) teaches associating https with port 443.

(2-c) The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem:

(2-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See the discussion at 1-c-1.

(2-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-2.

(2-c-3) During the years that have passed since Applicant first reduced Applicant's invention to practice and the years that have passed since Laurie was written, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(2-c-4) The Examiner failed to describe modifications to Laurie that in the view of the examiner both (i) would bring Laurie within the scope of Claim 4 and (ii) would have been obvious to one skilled in the art who was aware of Laurie, AOL and Apache and was confronted by the Firewall Problem. See the discussion at 1-c-4.

(2-d) The Examiner has provided no prior art to support the Examiner's view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Laurie to include, in combination, all of the elements of claim 4 that are missing from Laurie, including, inter alia: (2-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and (2-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext transfer protocol. Furthermore, the Examiner has failed to set forth modifications to Laurie that would bring Laurie within the scope of Claim 4. Applicant disagrees with the view that it would have been obvious to modify Laurie in some undisclosed way. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can both show support for this view and set forth a clear

description of changes to Laurie (obvious in light of AOL and Apache) that would bring Laurie within the scope of Claim 4.

In light of the foregoing discussion, Applicant respectfully requests that Claim 4 be allowed.

The **Third Issue** is whether the Examiner is justified in rejecting Claim 5-9 under 35 USC 103(a) as being unpatentable over Laurie as modified in accordance with AOL and Apache. Each of Claims 5-9 is dependent (directly or indirectly) from Claim 1. Consequently Each of Claims 5-9 is patentable if Claim 1 is patentable.

For the reasons set forth above with respect to Claim 1, Applicant respectfully requests that Claims 5-9 be allowed.

In light of the discussion above of the First through Third Issues, Applicant respectfully requests that claims 1-11 be allowed.

Respectfully submitted,

/s/

Carl Oppedahl
Attorney for Applicant
Reg. No. 32746
P.O. Box 5068
Dillon, CO 80435-5068
Telephone 970-468-6600